UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/754,802	01/09/2004	Hoe-Won Kim	678-1131	1597

66547 7590 07/22/2008

THE FARRELL LAW FIRM, P.C.
333 EARLE OVINGTON BOULEVARD
SUITE 701
UNIONDALE, NY 11553

EXAMINER	
PALIWAL, YOGESH	
ART UNIT	PAPER NUMBER
2135	
MAIL DATE	DELIVERY MODE
07/22/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/754,802	KIM, HOE-WON	
	Examiner	Art Unit	
	YOGESH PALIWAL	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 April 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-11* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-11* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

- Applicant's submission for RCE filed on April 21, 2008 has been entered.
- Applicant has added claim 11. Currently claims 1-11 are pending in this application.

Response to Arguments

1. Applicant's arguments with respect to claims 1-10 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 3, 6, 7, and 11 are rejected under 35 U.S.C. 102(e) as being anticipated by Bell et al. (US 2003/0130952 A1), hereinafter "Bell".

Regarding **Claim 3**, Bell discloses a data service providing apparatus for providing data requested by a communication terminal (see, Fig. 1, Numeral 20), comprising:

a data database for storing data (M) to be provided to the communication terminal (see, Fig. 1, Numeral 22);

a hidden secret key (user keys) database for storing a hidden secret key (Kh) corresponding to intrinsic identification information of a security deciphering module equipped in the communication terminal to decipher enciphered data (see, Fig. 6, Numeral 107);

a transmitting/receiving unit (see, Fig. 1, Numeral 20) for performing communication with the communication terminal (see, Fig. 1, Numerals 12, 18, 19) via a public network (see, Fig. 1, Numeral 14)

a data enciphering unit for enciphering the data (M) (content) by using a cipher key (Ks) (content key) (see, Fig. 7, Numeral 138 and also see paragraph 0047, "The content is then encrypted using a random content key 138") ;

a cipher key enciphering unit for enciphering the cipher key (Ks) by using the hidden secret key (Kh) (see, Fig. 9, Numeral 232 and also see paragraph 0058, "Once this selection is made, the process moves to the generation of a license through a process of encrypting the content key with the user key, and attaching a verification key 232."); and

a control unit for controlling the enciphering operations of the data and cipher key enciphering units (see, Fig. 9, Numerals 120, 124, 128, 130, 132, 136 and 138 and also see Fig. 9, Numeral 232), and

controlling the transmitting/receiving unit to provide the enciphered data ([M]Ks) and the personal secret key ([Ks]Kh) via the public network (see Paragraph 0052).

Regarding **Claim 6**, Bell discloses a security deciphering method comprising the steps of:

determining whether or not a personal secret key ([Ks]Kh) (encrypted content key), generated by enciphering a cipher key (Ks) by using a hidden secret key (Kh) (user key) corresponding to intrinsic identification information, is received (see, Paragraph 0059, "Particularly, the process moves to step 240 where the decision block checks if the license exits via the use of the broker")

if it is determined that the personal secret key ([Ks]Kh) is received, then decoding the received personal secret key ([Ks]Kh) by using the hidden secret key (Kh), thereby obtaining the cipher key (Ks) (see, Paragraph 0059, "When a license does exist, the content key is generated by decrypting the license with the user key 242")

determining whether or not enciphered data ([M]Ks), generated by enciphering data (M) requested to be transmitted by using the cipher key (Ks), is received (see, Fig. 9, Numerals, 234 and 236); and

if it is determined that the enciphered data ([M]Ks) is received, then decoding the enciphered data ([M]Ks) by using the cipher key Ks, thereby obtaining the data (M) (see Fig. 9, Numeral 244).

Regarding **Claim 7**, Bell discloses a data service providing method for providing data requested by a communication terminal, comprising the steps of:

receiving via a public network a request for transmission of data (M) from the communication terminal (see, Paragraph 0052, "then the process moves to step 210 where each electronic content in that market is checked to determine whether that particular user has access permissions to view the existence of that content.");

enciphering the data (M) (content) by using a cipher key (Ks) (content key) in response to the received data transmission request, thereby generating enciphered data ([M]Ks) (encrypted content) (see, Paragraph 0047, "The content is then encrypted using a random content key 138, which is stored in a system server 140.")

enciphering, in response to the received data transmission request, the cipher key (Ks) by using a hidden secret key (Kh) corresponding to intrinsic identification information assigned to a security enciphering module equipped in the communication terminal to decode the enciphered data ([M]Ks), thereby generating personal secret key ([Ks]Kh) (see Paragraph 0057, "the process moves to the generation of a license through a process of encrypting the content key with the user key")

transmitting the enciphered data ([M]Ks) and the personal secret key ([Ks]Kh) to the communication terminal via the public network (see, Paragraph 0058, "The user will then download the content and the license 234. ")

Regarding **Claim 11**, Bell discloses a security deciphering method comprising:

providing a hidden secret key (Kh) (user key) corresponding to intrinsic identification information (see, Fig. 6, Numeral 106, "Create unique user key");

providing a cipher key (Ks) (content key) (see, Fig. 7, Numeral 140);

generating a personal secret key ({Ks}Kh) (encrypted content key) by the cipher key (Ks) (content key) by using the hidden secret key (Kh) (user key) (see, Fig. 9, Numeral 232); and

encoding/decoding data M using the hidden secret key (Kh), the cipher key (Ks); and the personal secret key ({Ks} Kh), thereby achieving improved security for transmitting/receiving the data M over public networks (see, Paragraph 0059).

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 2, 4, 5, 8, 9 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bell in view of Bird (US 5,369,705), hereinafter "Bird".

Regarding **Claim 1**, Bell discloses a security deciphering apparatus comprising:

a first decoding unit for receiving via a public network a personal secret key ([Ks]Kh) (encrypted content key), generated by enciphering a cipher key (Ks) (content key) by using the hidden secret key (Kh) ("user key", see paragraph 0058, "the process moves to the generation of a license through a process of encrypting the content key with the user key"), and decoding the personal secret key ([Ks]Kh) (encrypted content key) by using the hidden secret key (Kh) (user key), thereby obtaining the cipher key (Ks) (content key) (see, Fig. 9, numeral 242 and also see paragraph 0059) and

a second decoding unit for receiving via the public network enciphered data ([M]Ks) (encrypted content) (see, Fig. 9, Numeral 244 and also see paragraph 0059), generated by enciphering data (M) (content) by using the cipher key (Ks) (content key) (see, Paragraph 0047, "The content is then encrypted using a random content key 138"), and decoding the enciphered data ([M]Ks) (encrypted content) by using the cipher key (Ks) (content key), thereby obtaining the data (M) (content) (see, Fig. 9, numeral 244, "the content is decrypted through use of the content key").

Bell discloses that user uses user key corresponding to intrinsic identification information to decrypt content key however, Bell does not explicitly disclose a storage unit that store a hidden secret key (user key).

Bird (US 5,369,705) discloses hidden secret key storing unit for storing a hidden secret key (see, Column 3, lines 58-60, "The user (A) also has the user's key (Ka) stored in its safe storage device (encrypted file, special hardware, a smart card, etc.).").

Therefore, it would have been obvious at the time invention was made to one of ordinary skill in the art to store, the user key of Bell, into a safe storage device such as smart card as taught by Bird because smart card provides a temper resistant hardware to safely protect the user key.

Regarding **Claim 2**, Rejection of claim 1 is incorporated and the combination of Bell and Bird further discloses:

a personal secret key (encrypted content key) storing unit for storing the personal secret key ([Ks]Kh) received via the public network (see Bell, Paragraph It is to be noted that the generated license in step 232 is downloaded to the computer of the user.) and

outputting the stored personal secret key ([Ks]Kh) to the first decoding unit under a control of the first decoding unit (see Bell, Fig. 9, Numeral 242); and

a cipher key storing unit for storing the cipher key (Ks) obtained by the first decoding unit (see Bell, Fig. 9, Numeral 242, since the decryption process of the content key is taking place in user's computer, it is implied that that cipher key is stored (even temporarily) into the computer of the user to perform the content decryption), and

outputting the stored cipher key (Ks) to the second decoding unit under a control of the second decoding unit (see Bell, Fig. 9, Numeral 244).

Regarding **Claim 4**, the rejection of claim 3 is incorporated and Bell further discloses that security deciphering module comprises:

a first decoding unit for receiving via a public network a personal secret key ([Ks]Kh) (encrypted content key), generated by enciphering a cipher key (Ks) (content key) by using the hidden secret key (Kh) ("user key", see paragraph 0058, "the process moves to the generation of a license through a process of encrypting the content key with the user key"), and decoding the personal secret key ([Ks]Kh) (encrypted content key) by using the hidden secret key (Kh) (user key), thereby obtaining the cipher key (Ks) (content key) (see, Fig. 9, numeral 242 and also see paragraph 0059) and

a second decoding unit for receiving via the public network enciphered data ([M]Ks) (encrypted content) (see, Fig. 9, Numeral 244 and also see paragraph 0059), generated by enciphering data (M) (content) by using the cipher key (Ks) (content key) (see, Paragraph 0047, "The content is then encrypted using a random content key 138"), and decoding the enciphered data ([M]Ks) (encrypted content) by using the cipher key (Ks) (content key), thereby obtaining the data (M) (content) (see, Fig. 9, numeral 244, "the content is decrypted through use of the content key").

Bell discloses that user uses user key corresponding to intrinsic identification information to decrypt content key however, Bell does not explicitly disclose a storage unit that store a hidden secret key (user key).

Bird discloses hidden secret key storing unit for storing a hidden secret key (see, Column 3, lines 58-60, "The user (A) also has the user's key (Ka) stored in its safe storage device (encrypted file, special hardware, a smart card, etc.).").

Therefore, it would have been obvious at the time invention was made to one of ordinary skill in the art to store, the user key of Bell, into a safe storage device such as smart card as taught by Bird because smart card provides a temper resistant hardware to safely protect the user key.

Regarding **Claim 5**, the rejection of claim 4 is incorporated and the combination of Bell and Bird further discloses:

a personal secret key (encrypted content key) storing unit for storing the personal secret key ([Ks]Kh) received via the public network (see Bell, Paragraph It is to be noted that the generated license in step 232 is downloaded to the computer of the user.) and

outputting the stored personal secret key ([Ks]Kh) to the first decoding unit under a control of the first decoding unit (see Bell, Fig. 9, Numeral 242); and

a cipher key storing unit for storing the cipher key (Ks) obtained by the first decoding unit (see Bell, Fig. 9, Numeral 242, since the decryption process of the content key is taking place in user's computer, it is implied that that cipher key is stored (even temporarily) into the computer of the user to perform the content decryption), and

outputting the stored cipher key (Ks) to the second decoding unit under a control of the second decoding unit (see Bell, Fig. 9, Numeral 244).

Regarding **Claim 8**, rejection of claim 7 above is incorporated and further Bell discloses, that the security enciphering module equipped in the communication terminal comprises:

a first decoding unit for receiving via a public network a personal secret key ([Ks]Kh) (encrypted content key), generated by enciphering a cipher key (Ks) (content key) by using the hidden secret key (Kh) ("user key", see paragraph 0058, "the process moves to the generation of a license through a process of encrypting the content key with the user key"), and decoding the personal secret key ([Ks]Kh) (encrypted content key) by using the hidden secret key (Kh) (user key), thereby obtaining the cipher key (Ks) (content key) (see, Fig. 9, numeral 242 and also see paragraph 0059) and

a second decoding unit for receiving via the public network enciphered data ([M]Ks) (encrypted content) (see, Fig. 9, Numeral 244 and also see paragraph 0059), generated by enciphering data (M) (content) by using the cipher key (Ks) (content key) (see, Paragraph 0047, "The content is then encrypted using a random content key 138"), and decoding the enciphered data ([M]Ks) (encrypted content) by using the cipher key (Ks) (content key), thereby obtaining the data (M) (content) (see, Fig. 9, numeral 244, "the content is decrypted through use of the content key").

Bell discloses that user uses user key corresponding to intrinsic identification information to decrypt content key however, Bell does not explicitly disclose a storage unit that store a hidden secret key (user key).

Bird discloses hidden secret key storing unit for storing a hidden secret key (see, Column 3, lines 58-60, "The user (A) also has the user's key (Ka) stored in its safe storage device (encrypted file, special hardware, a smart card, etc.).").

Therefore, it would have been obvious at the time invention was made to one of ordinary skill in the art to store, the user key of Bell, into a safe storage device such as smart card as taught by Bird because smart card provides a temper resistant hardware to safely protect the user key.

Regarding **Claim 9**, rejection of claim 8 is incorporated and the combination of Bell and Bird further discloses:

a personal secret key (encrypted content key) storing unit for storing the personal secret key ([Ks]Kh) received via the public network (see Bell, Paragraph It is to be noted that the generated license in step 232 is downloaded to the computer of the user.) and

outputting the stored personal secret key ([Ks]Kh) to the first decoding unit under a control of the first decoding unit (see Bell, Fig. 9, Numeral 242); and

a cipher key storing unit for storing the cipher key (Ks) obtained by the first decoding unit (see Bell, Fig. 9, Numeral 242, since the decryption process of the content key is taking place in user's computer, it is implied that that cipher key is stored (even temporarily) into the computer of the user to perform the content decryption), and

outputting the stored cipher key (Ks) to the second decoding unit under a control of the second decoding unit (see Bell, Fig. 9, Numeral 244).

Regarding **Claim 10**, Bell discloses in a mobile communication terminal receiving, via a public network, enciphered data ([M]Ks) (encrypted content) generated by enciphering data (M) (content) by using a cipher key (Ks) (content key), a security deciphering apparatus comprising:

a first decoding unit for receiving a personal secret key ([Ks]Kh), generated by enciphering a cipher key (Ks) by using the hidden secret key (Kh) ("user key", see paragraph 0058, "the process moves to the generation of a license through a process of encrypting the content key with the user key"), and decoding the personal secret key ([Ks]Kh) by using the hidden secret key (Kh), thereby obtaining the cipher key (Ks) (see, Fig. 9, numeral 242 and also see paragraph 0059); and

a second decoding unit for decoding the enciphered data ([M]Ks) (see, Fig. 9, Numeral 244 and also see paragraph 0059) by using the obtained cipher key (Ks) (see, Paragraph 0047, "The content is then encrypted using a random content key 138"), thereby obtaining the data (M) (see, Fig. 9, numeral 244, "the content is decrypted through use of the content key").

Bell discloses that user uses user key corresponding to intrinsic identification information to decrypt content key however, Bell does not explicitly disclose a storage unit that store a hidden secret key (user key).

Bird discloses hidden secret key storing unit for storing a hidden secret key (see, Column 3, lines 58-60, "The user (A) also has the user's key (Ka) stored in its safe storage device (encrypted file, special hardware, a smart card, etc.).").

Therefore, it would have been obvious at the time invention was made to one of ordinary skill in the art to store, the user key of Bell, into a safe storage device such as smart card as taught by Bird because smart card provides a temper resistant hardware to safely protect the user key.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to YOGESH PALIWAL whose telephone number is (571)270-1807. The examiner can normally be reached on M-F: 7:30 AM - 5:00 PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Y. P./
Examiner, Art Unit 2135

/H. S./

Primary Examiner, Art Unit 2135